



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/764,683	01/18/2001	Fabrice Walter	ICB-0038	6920

29116 7590 05/07/2004

ROBINSON & POST, L.L.P.
NORTH DALLAS BANK TOWER, SUITE 575
12900 PRESTON ROAD, LB-41
DALLAS, TX 75230

EXAMINER

WU, ALLEN S

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 05/07/2004

4

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/764,683

Applicant(s)

WALTER ET AL.

Examiner

Allen S. Wu

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 January 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 January 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 2.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
2. Claims 7-10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
3. Claims 7 and 8 recites the word "them." There is a lack of clarification as to what "them" refers to in the claim. Appropriate correction is required. Claims 9-10 are dependents of claim 7 and inherit the same reasons of rejection.

Priority

4. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Drawings

5. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: 18 of fig 1. A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the

Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

- (a) TITLE OF THE INVENTION.
- (b) CROSS-REFERENCE TO RELATED APPLICATIONS.
- (c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
- (d) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or
REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)
- (e) BACKGROUND OF THE INVENTION.
 - (1) Field of the Invention.
 - (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
- (f) BRIEF SUMMARY OF THE INVENTION.
- (g) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
- (h) DETAILED DESCRIPTION OF THE INVENTION.
- (i) CLAIM OR CLAIMS (commencing on a separate sheet).
- (j) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
- (k) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1, 5-8, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geronimi et al (hereinafter Geronimi), US Patent 5,629,513, in view of Yu et al (hereinafter Yu), US Patent 6,067,621.

As per claim 1, Geronimi et al discloses a method of testing an integrated circuit containing hardware and/or software parts having a confidential nature (see for example, col 2 ln 60-62) wherein the method comprises: sending parameters to an integrated circuit (see for example; col 4 ln 50-55) comparing first and second parameters (see for example; col 2 ln 51-60 and col 4 ln 44-49), wherein the parameters are calculated by a ciphering algorithm (see for example; encryption col 4 ln 50-55), and freeing a test path leading from a tester to parts of a confidential nature, only if the comparison establishes a match between said first and second parameters (see for example; col 4 ln 44-65 and col 5 ln 1-4).

Geronimi does not explicitly teach the use of a first and second password being generated from a random number. Yu discloses an authentication means comprising of generating a random number (see for example; col 8 ln 25-27); ciphering this random number using a key stored in said integrated circuit via a

Art Unit: 2135

ciphering algorithm to obtain a first password (see for example; col 6 ln 47-60); sending the random number (see for example; col 10 ln 31-37 and 43-52); ciphering in parallel said random number received using a key identical to that used in said integrated circuit (see for example col 7 ln 40-58 and col 10 ln 1-17) via an identical ciphering algorithm to that implemented in said integrated circuit, to generate a second password (see for example; col 7 ln 40-56). Geronimi recognizes the need of authentication before freeing a test path (see for example; col 4 ln 56-col 5 ln 4). Yu further discloses a means of authentications between a communications device (server) and an integrated circuit (see for example; IC card, abstract). Furthermore, authentications schemes are well known in the art to capable to be implemented by any means depending of which system is doing the authentication. One of ordinary skill in the art at the time of the applicant's invention would have recognized the case of the integrated circuit doing the authenticating in Geronimi and used the authentication communication means of Yu for authenticating a tester, wherein a random number is sent from the integrated circuit to the tester and passwords are received and compared by the integrated circuit. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Yu within Geronimi because it would have increased access security through the use of one-time-passwords based on a random number (see for example; Yu col 2 ln 1-13).

As per claim 5, Geronimi-Yu discloses the claimed limitations as described above (see claim 1). Yu further discloses checking whether said received and calculated random numbers are equal (see for example; col 4 ln 63-65; the passwords are calculated using the same algorithm, therefore checking the passwords are essentially checking for a match in the random numbers).

As per claim 6, Geronimi-Yu discloses the claimed limitations as described above (see claim 1). Yu further discloses a means of storing a predetermined value of said cipher key (see for example; col 12 ln 1-24). As for checking whether a cipher key sent has the predetermined value stored in said integrated circuit, commanding said key sent to be stored in said integrated circuit in case an inequality is observed during said check and blocking such case the storage in said circuit of any other cipher key, Yu further discloses an alternative means of such insertion of a cipher key wherein a service provider is inserts the key at registration. Both the means disclosed by Yu and the claimed limitations include are means of initializing the integrated circuit with the cipher key. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to have a design choice in initializing a cipher key because the applicant has not explicitly stated any reason or purpose for such a checking and blocking means other than loading a cipher key into an integrated circuit and the means of Geronimi-Yu is just as efficient.

As per claim 7, Geronimi et al discloses an integrated circuit containing hardware and/or software parts having a confidential nature (see for example, col 2 ln 60-62) wherein the integrated circuit comprises: means of comparing first parameter and a second received parameter (see for example; col 2 ln 51-60 and col 4 ln 44-49), wherein the parameters are calculated by a ciphering algorithm (see for example; encryption col 4 ln 50-55)

Geronimi does not explicitly teach a first password generated from a random number. Yu discloses an authentication means comprising of generating a random number (see for example; col 8 ln 25-27); storing a cipher key (see for example; col 6 ln 15-16); ciphering this random number using a key stored in said integrated circuit via a ciphering algorithm to obtain a first password (see for example; col 6 ln 47-60); and comparing a first password with a second password received from the exterior (see for example col 8 ln 10-16), said second password being calculated in accordance with the random number generated by the generator (see for example; col 7 ln 40-67). Geronimi recognizes the need of authentication (see for example; col 4 ln 56-col 5 ln 4). Yu further discloses a means of authentications between a communications device (server) and an integrated circuit (see for example; IC card, abstract). Furthermore, authentication schemes are well known in the art to capable to be implemented by any means depending of which system is doing the authentication. One of ordinary skill in the art at the time of the applicant's invention would have recognized the case of the integrated circuit doing the

authenticating in Geronimi and used the authentication communication means of Yu for authenticating a tester, wherein a random number is sent from the integrated circuit to the tester and passwords are received and compared by the integrated circuit. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Yu within Geronimi because it would have increased access security through the use of one-time-passwords based on a random number (see for example; Yu col 2 ln 1-13).

As per claim 8, Geronimi-Yu discloses the claimed limitations as disclosed above (see claim 7). Geronimi further discloses means for storing a first parameter, said storage means being placed before the comparison means to provide the said first password at the moment of comparison with the second password (see for example col 2 ln 51-59 and col 4 ln 50-65; such storing of a computed value must be done prior to comparison).

As per claim 11, Geronimi et al discloses a tester for an integrated circuit containing hardware and/or software parts having a confidential nature (see for example, col 2 ln 60-62; a tester be present to run such testing of the integrated circuit) wherein the tester comprises: means of sending (routing) a calculated parameter to an integrated circuit (see for example; col 4 ln 34-55).

Geronimi does not explicitly teach a second password generated from a received random number. Yu discloses an authentication means comprising of storing a cipher key (see for example; col 6 ln 15-16); ciphering this random number using a key stored in said tester via a ciphering algorithm to obtain a second password (see for example; col 7 ln 40-67). Geronimi recognizes the need of authentication (see for example; col 4 ln 56-col 5 ln 4). Yu further discloses a means of authentications between a communications device (server) and an integrated circuit (see for example; IC card, abstract). Furthermore, authentication schemes are well known in the art to capable to be implemented by any means depending of which system is doing the authentication. One of ordinary skill in the art at the time of the applicant's invention would have recognized the case of the integrated circuit doing the authenticating in Geronimi and used the authentication communication means of Yu for authenticating a tester, wherein a random number is sent from the integrated circuit to the tester and passwords are received and compared by the integrated circuit. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Yu within Geronimi because it would have increased access security through the use of one-time-passwords based on a random number (see for example; Yu col 2 ln 1-13).

8. Claims 2-3, 10, and 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geronimi et al (hereinafter Geronimi), US Patent 5,629,513, in view

of Yu et al (hereinafter Yu), US Patent 6,067,621, as applied to claim 1 above, and further in view of Lewis, US Patent 5,875,248.

As per claims 2 and 12, Geronimi-Yu discloses the claimed limitations as described above (see claim 1). Yu further discloses the ciphering of random numbers using a key stored in the integrated circuit via said ciphering algorithm to obtain another password (see for example; password is changed col 2 ln 1-14). By the synchronization scheme of Yu, one of ordinary skill in the art at the time of the applicant's invention would have recognized the further generation of passwords in the tester using a key (see for example; col 8 ln 1-8). The Geronimi-Yu combination does not explicitly teach authorizing the ciphering of said second password via said tester only if there is a match between said third and fourth passwords. Lewis further discloses a means of authentication between an integrated circuit and a communication device (see for example; abstract and col 3 ln 1-14) wherein a device receives a third password (PIN) and comparing said third and fourth passwords (see for example; col 9 ln 19-22) and authorizing the ciphering of a second password if there is a match between said third and fourth passwords (col 9 ln 19-46). Both Lewis and the Geronimi-Yu combination disclose a means of authentication between an integrated circuit and a second device for accessing a part of the integrated circuit. By providing an extra layer of authentication before ciphering of the second password, access security is further increased (see for example; Lewis col 5 ln 61-col 6 ln 4). Lewis further discloses that the PIN is created based on a unique identifier (see for

example; col 8 ln 1-15). One of ordinary skill in the art at the time of the applicant's invention would have realized the generation of third and fourth passwords based on the password generation means of Geronimi-Yu and further applying the comparison between the passwords by the comparison means of Lewis in implementing such a combination .It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Lewis within the Geronimi-Yu combination because it would have provided an extra layer of security due to another variable in authenticating between two devices.

As per claims 3 and 13, As per claim 2, Geronimi-Yu discloses the claimed limitations as described above (see claim 1). Yu further discloses the ciphering of random numbers using a key stored in the integrated circuit via said ciphering algorithm to obtain another password (see for example; password is changed col 2 ln 1-14). By the synchronization scheme of Yu, one of ordinary skill in the art at the time of the applicant's invention would have recognized the further generation of passwords in the tester using a key (see for example; col 8 ln 1-8). The Geronimi-Yu combination does not explicitly teach authorizing the ciphering of said second password via said tester only if there is a match between said third and fourth passwords. Lewis further discloses a means of authentication between an integrated circuit and a communication device (see for example; abstract and col 3 ln 1-14) wherein a device receives a third password

(PIN) and performing the reverse ciphering of said third password received, using key stored in the tester (smart chip) via said ciphering algorithm to find a PIN (see for example; col 8 ln 16-37) and authorizing the ciphering of a second password if there is a match between said the PIN stored and a calculated PIN (col 8 ln 16-37). Both Lewis and the Geronimi-Yu combination disclose a means of authentication between an integrated circuit and a second device for accessing a part of the integrated circuit. By providing an extra layer of authentication before ciphering of the second password, access security is further increased (see for example; Lewis col 5 ln 61-col 6 ln 4). One of ordinary skill in the art at the time of the applicant's invention would have realized the generation of third password based on the password generation means of Geronimi-Yu and further applying the comparison between the random numbers by the comparison means of Lewis in implementing such a combination. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Lewis within the Geronimi-Yu combination because it would have provided an extra layer of security due to another variable in authenticating between two devices.

As per claim 10, Geronimi-Yu discloses the claimed limitations described above (see claim 7). Yu further discloses the ciphering of random numbers using a key stored in the integrated circuit via said ciphering algorithm to obtain another password (see for example; password is changed col 2 ln 1-14). By the

synchronization scheme of Yu, one of ordinary skill in the art at the time of the applicant's invention would have recognized the further generation of passwords in the tester using a key (see for example; col 8 ln 1-8). Geronimi-Yu does not explicitly teach sending a third password with a generated random number. Lewis further discloses a means of authentication between an integrated circuit and a communication device (see for example; abstract and col 3 ln 1-14) wherein a device receives a third password (PIN) and comparing said third and fourth passwords (see for example; col 9 ln 19-22) and authorizing the ciphering of a second password if there is a match between said third and fourth passwords (col 9 ln 19-46). Both Lewis and the Geronimi-Yu combination disclose a means of authentication between an integrated circuit and a second device for accessing a part of the integrated circuit. By providing an extra layer of authentication before ciphering of the second password, access security is further increased (see for example; Lewis col 5 ln 61-col 6 ln 4). Lewis further discloses that the PIN is created based on a unique identifier (see for example; col 8 ln 1-15). One of ordinary skill in the art at the time of the applicant's invention would have realized the generation of third and fourth passwords based on the password generation means of Geronimi-Yu and further applying the comparison between the passwords by the comparison means of Lewis in implementing such a combination. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Lewis within the Geronimi-Yu combination because it would have provided an

extra layer of security due to another variable in authenticating between two devices. Furthermore, for simplicity of the system, one of ordinary skill in the art at the time of the applicant's invention would have realized the use of the same random number for generating a third password to reduce the amount of number generated which will increase the need of further synchronizing.

9. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Geronimi et al (hereinafter Geronimi), US Patent 5,629,513, in view of Yu et al (hereinafter Yu), US Patent 6,067,621, in view of Lewis, US Patent 5,875,248, and further in view of Fukawa, US Patent 6,112,187.

As per claim 4, Geronimi-Yu-Lewis discloses the claimed limitations as described above (see claims 2 and 3). Geronimi-Yu-Lewis does not explicitly teach a means of ciphering said third and/or fourth passwords made on the basis of different number of clock strokes than that used for ciphering said first and second passwords. Fukawa discloses a means of ciphering made on the basis of different number of clock strokes (see for example; col 9 ln 65-col 10 ln 10). The ciphering made on the basis of different number of clock strokes is well known in the art to provide a means of generating a time-varying encryption scheme, thus further prohibiting the attack on the encryption algorithm. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Fukawa within the Geronimi-Yu-Lewis

combination because it would have provided greater security on attacks to the ciphering algorithm between data.

10. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Geronimi et al (hereinafter Geronimi), US Patent 5,629,513, in view of Yu et al (hereinafter Yu), US Patent 6,067,621, and further in view of Bonneau et al (hereinafter Bonneau), US Patent 6,577,229.

As per claim 9, Geronimi-Yu discloses the claimed limitations as described (see claim 7). Yu further discloses a memory for storing a cipher key (see for example col 6 ln 15-17). Geronimi-Yu do not explicitly teach an EEPROM memory which also includes a redundancy check unit. Bonneau discloses device which uses EEPROM, which includes a redundancy check unit for storage and verification of data (see for example col 11 ln 23-33). EEPROM are well known in the art to be used as a memory in compact devices and integrated circuits. The use of cyclic redundancy code is well known in the art to be used for error detection and correction of data. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Bonneau within the Geronimi-Yu combination because it would have provided reliable data transmission and storage through the use of EEPROM and cyclic redundancy for the storage of such critical data, such as keys.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent 4,802,217, to Michener discloses a means of controlling access to a computer through the use of ciphering.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Allen S. Wu whose telephone number is 703-305-0708. The examiner can normally be reached on Monday-Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Allen Wu
Patent Examiner
Art Unit 2135

ASW


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100